W1505

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-016418
(43)Date of publication of application : 17.01.2003

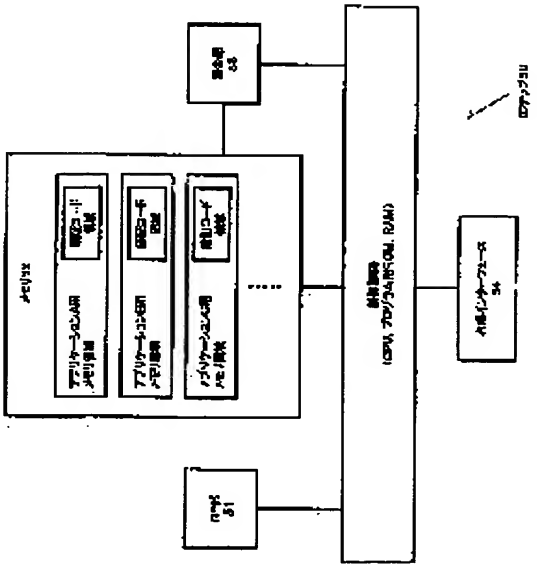
(51)Int.Cl. G06K 19/10
B42D 15/10
G06F 12/00
G06F 12/14
G06K 19/07

(21)Application number : 2001-194749
(22)Date of filing : 27.06.2001

(71)Applicant : SONY CORP
(72)Inventor : YAMAGATA AKIHIKO
FUKADA AKIRA

## (54) PORTABLE TERMINAL AND ITS CONTROL METHOD, AND IC CARD

(57)Abstract:
PROBLEM TO BE SOLVED: To efficiently control the right to access each application allocated to a memory area of an IC card.
SOLUTION: By introducing a hierarchical structure to memory areas on the IC card, respective applications allocated to the memory areas are registered in directories, and the memory areas are managed by directories. Password codes are set for every application and directory and the right to access is controlled in the application units and directory units. If a portable terminal is lost, the right to access the applications in the IC card is automatically lost.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

W1608

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－16418
（P2003－16418A）
(43)公開日　平成15年１月17日(2003.1.17)

| (51)Int.Cl.[7] | | 識別記号 | FI | | テーマコード(参考) | |
|---|---|---|---|---|---|---|
| Ｇ０６Ｋ | 19/10 | | Ｂ４２Ｄ | 15/10 | ５２１ | ２Ｃ００５ |
| Ｂ４２Ｄ | 15/10 | ５２１ | Ｇ０６Ｆ | 12/00 | ５３７Ｄ | ５Ｂ０１７ |
| Ｇ０６Ｆ | 12/00 | ５３７ | | 12/14 | ３２０Ｃ | ５Ｂ０３５ |
| | 12/14 | ３２０ | Ｇ０６Ｋ | 19/00 | Ｒ | ５Ｂ０８２ |
| Ｇ０６Ｋ | 19/07 | | | | Ｈ | |

審査請求　未請求　請求項の数18　ＯＬ　（全 17 頁）

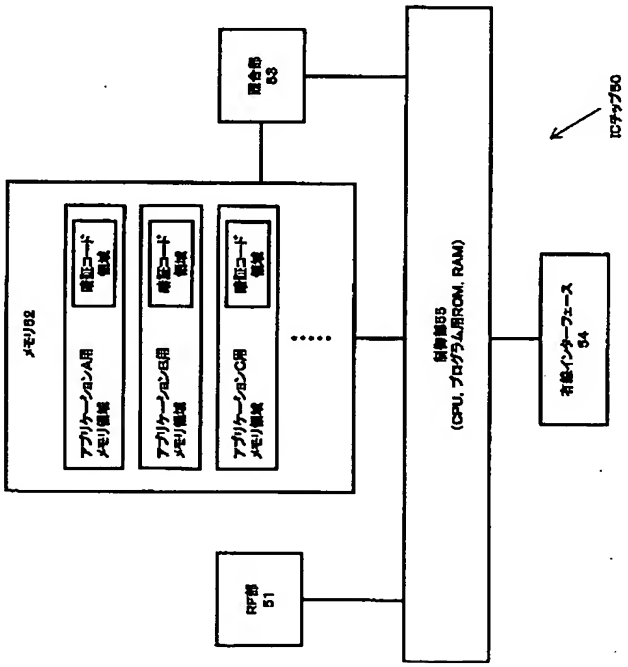
(21)出願番号　特願2001－194749(P2001－194749)
(22)出願日　平成13年６月27日(2001.6.27)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　山形　昭彦
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　深田　顕
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

最終頁に続く

(54)【発明の名称】　携帯端末及びその制御方法、並びに、ＩＣカード

(57)【要約】
【課題】　ＩＣカードのメモリ領域に割り当てられた各アプリケーションへのアクセス権を効率的に制御する。
【解決手段】　ＩＣカード上のメモリ領域に階層構造を導入することにより、メモリ領域上に割り当てられた各アプリケーションをディレクトリに登録して、ディレクトリ毎にメモリ領域を管理する。アプリケーション毎、並びにディレクトリ毎に暗証コードを設定して、アプリケーション単位又はディレクトリ単位でアクセス権を制御する。また、携帯端末を紛失した場合には、ＩＣカード内のアプリケーションへのアクセス権が自動的に消失する。



【特許請求の範囲】
【請求項１】外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたＩＣチップを搭載した携帯端末であって、
前記ＩＣチップ上のメモリ領域に割り当てられた、暗証コードによりアクセス権が制御された１以上のアプリケーションと、
前記ＩＣチップが外部機器と無線通信するための無線インターフェースと、
前記携帯端末内で前記ＩＣチップと有線通信するための有線インターフェースと、
ユーザが暗証コードその他のデータを入力することができるユーザ入力手段と、
前記ユーザ入力手段から入力された暗証コード前記有線インターフェースを介して前記ＩＣチップに転送して、
前記ＩＣチップ上のメモリ領域に割り当てられた各アプリケーションの暗証コードと比較照合する照合手段と、
前記照合手段による比較照合の結果、暗証コードが一致するアプリケーションに関するアクセス権をユーザに与えるアクセス権制御手段と、を具備することを特徴とする携帯端末。
【請求項２】前記アクセス権制御手段は、アクセス権が与えられたアプリケーションに対する外部機器からの前記無線インターフェースを介した無線通信によるアクセスを許容する、ことを特徴とする請求項１に記載の携帯端末。
【請求項３】前記アクセス権制御手段は、前記無線インターフェース経由で接続された外部機器からの電波を検出しなくなったことに応答して、アクセス権を付与したアプリケーションに関する一連のトランザクションが終了したと判断して、トランザクション終了処理を行なう、ことを特徴とする請求項１に記載の携帯端末。
【請求項４】前記アクセス権制御手段は、前記ＩＣチップから前記無線インターフェース経由で送出したコマンドに対するレスポンスが所定時間内に受信されなかったことに応答して、前記無線インターフェース経由で接続された外部機器と前記ＩＣチップとの一連のトランザクションが正常又は異常終了したとみなして、終了処理を行なう、ことを特徴とする請求項１に記載の携帯端末。
【請求項５】アプリケーション毎にあらかじめ暗証コードを登録する暗証コード登録手段と、
プログラム起動手段と、
起動されたプログラムに応じて該当するアプリケーションに対応する暗証コードを前記有線インターフェース経由で前記ＩＣチップに入力する暗証コード入力手段と、をさらに備えることを特徴とする請求項１に記載の携帯端末。
【請求項６】前記ＩＣチップは、
前記無線インターフェース経由で外部機器に接続されて給電されたことに応答して、前記ＩＣチップ上のメモリ領域にアクセスするために暗証コードの入力が必要である旨を前記有線インターフェース経由で通知する、ことを特徴とする請求項１に記載の携帯端末。
【請求項７】外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたＩＣチップを搭載した携帯端末の制御方法であって、
前記携帯端末は、前記ＩＣチップが外部機器と無線通信するための無線インターフェースと、前記携帯端末内で前記ＩＣチップと有線通信するための有線インターフェースとを備え、
前記ＩＣチップ上のメモリ領域には暗証コードによりアクセス権が制御された１以上のアプリケーションが割り当てられており、
ユーザから暗証コードを入力するユーザ入力ステップと、
前記ユーザ入力ステップにより入力された暗証コードを前記有線インターフェース経由で前記ＩＣチップに送出するステップと、
前記ＩＣチップ上のメモリ領域に割り当てられた各アプリケーションの暗証コードと、前記ユーザ入力ステップにより入力された暗証コードとを比較照合する照合ステップと、
前記照合ステップにおける比較照合の結果、暗証コードが一致するアプリケーションに関するアクセス権をユーザに与えるアクセス権制御ステップと、を具備することを特徴とする携帯端末の制御方法。
【請求項８】前記アクセス権制御ステップでは、アクセス権が与えられたアプリケーションに対する外部機器からの前記無線インターフェースを介した無線通信によるアクセスを許容する、ことを特徴とする請求項７に記載の携帯端末の制御方法。
【請求項９】前記アクセス権制御ステップでは、前記インターフェース経由で接続された外部機器からの電波を検出しなくなったことに応答して、アクセス権を付与したアプリケーションに関する一連のトランザクションが終了したと判断して、トランザクション終了処理を行なう、ことを特徴とする請求項７に記載の携帯端末の制御方法。
【請求項１０】前記アクセス権制御ステップでは、前記ＩＣチップから前記無線インターフェース経由で送出したコマンドに対するレスポンスが所定時間内に受信されなかったことに応答して、前記無線インターフェース経由で接続された外部機器と前記ＩＣチップとの一連のトランザクションが正常又は異常終了したとみなして、終了処理を行う、ことを特徴とする請求項７に記載の携帯端末の制御方法。
【請求項１１】アプリケーション毎にあらかじめ暗証コードを登録する暗証コード登録ステップと、
プログラム起動ステップと、
起動されたプログラムに応じて該当するアプリケーショ

ンに対応する暗証コードを前記有線インターフェース経由で前記ＩＣチップに入力する暗証コード入力ステップと、をさらに備えることを特徴とする請求項７に記載の携帯端末の制御方法。

【請求項１２】前記ＩＣチップが前記無線インターフェース経由で外部機器に接続されて給電されたことに応答して、前記ＩＣチップ上のメモリ領域にアクセスするために暗証コードの入力が必要である旨を前記有線インターフェース経由で通知するステップをさらに備える、ことを特徴とする請求項７に記載の携帯端末の制御方法。

【請求項１３】携帯端末に付随して使用されるＩＣカードであって、

外部機器と無線通信するための無線インターフェースと、

前記携帯端末と有線通信するための有線インターフェースと、

暗証コードによりアクセス権が制御された１以上のアプリケーションが割り当てられたメモリ領域と、を具備し、前記無線インターフェース経由で外部機器に接続されたことに応答して給電されて駆動する、ことを特徴とするＩＣカード。

【請求項１４】前記無線インターフェース経由で受信した暗証コードが一致したことに応答して、メモリ領域上の対応するアプリケーションのアクセス権が前記無線インターフェース経由で接続された外部機器に与えられる、ことを特徴とする請求項１３に記載のＩＣカード。

【請求項１５】前記有線インターフェース経由で受信した暗証コードが一致したことに応答して、メモリ領域上の対応するアプリケーションのアクセス権が前記無線インターフェース経由で接続された外部機器に与えられる、ことを特徴とする請求項１３に記載のＩＣカード。

【請求項１６】前記無線インターフェース経由で接続された外部機器からの電波を検出しなくなったことに応答して、該外部機器に与えられているアプリケーションへのアクセス権が失効する、ことを特徴とする請求項１３に記載のＩＣカード。

【請求項１７】前記無線インターフェース経由で送出したコマンドに対するレスポンスが所定時間内に受信されなかったことに応答して、該外部機器に与えられているアプリケーションへのアクセス権が失効する、ことを特徴とする請求項１３に記載のＩＣカード。

【請求項１８】前記無線インターフェース経由で外部機器に接続されて給電されて駆動することに応答して、前記ＩＣチップ上のメモリ領域にアクセスするために暗証コードの入力が必要である旨を前記有線インターフェース経由で通知する、ことを特徴とする請求項１３に記載のＩＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、外部機器との無線通信により給電されて駆動するＩＣチップを搭載した携帯端末、並びに、携帯端末に付随して使用されるＩＣカードに係り、特に、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたＩＣチップを搭載した携帯端末及びその制御方法、並びに、メモリ機能を備えたＩＣカードに関する。

【０００２】更に詳しくは、本発明は、ＩＣチップ上のメモリ領域に１以上のアプリケーションが割り当てられた携帯端末及びその制御方法、並びに、メモリ領域に１以上のアプリケーションが割り当てたＩＣカードに係り、特に、ＩＣチップ上のメモリ領域に割り当てられた各アプリケーション毎にアクセス権を制御する携帯端末及びその制御方法、並びに、メモリ領域に割り当てられた各アプリケーション毎にアクセス権を制御するＩＣカードに関する。

【０００３】

【従来の技術】従来から、本人確認や認証処理のために暗証番号やパスワードを用いたさまざまな装置が考案され、実用に供されている。（ここで、一般に、「暗証番号」とは０から９までの数字の組み合わせで表される文字列のことを言い、また、「パスワード」は、数字に加えてアルファベットなどの一般文字を用いて表される文字列のことを言う。本明細書中では、暗証番号とパスワードを併せて「暗証コード」とも呼ぶ。）

【０００４】例えば、銀行やその他の金融機関において、キャッシュ･カードを使用する際には、キャッシュ･ディスペンサなどで、本人認証の手段として、暗証番号やパスワードの入力を使用者に対して促し、使用者から正しい暗証番号やパスワードが入力されたことを確認してから、キャッシュ･ディスペンサなどから出金動作を行なうようになっている。

【０００５】この他にも、ホテルなどの宿泊施設に設置されたセーフティ･ボックスの暗礁コード入力、コンピュータへのログイン時のパスワード入力、あるいは情報端末上の情報を秘匿するためなど、暗証コードに関する適用例はさまざまである。

【０００６】従来、１枚の銀行用キャッシュ･カード上に配設されている磁気ストライプなどの記憶媒体の中には、その銀行に対してのみ使用可能な記憶領域しか設けられていない。したがって、上述したような暗証番号あるいはパスワードの入力は、この単一の記憶領域へのアクセスに過ぎない。したがって、ユーザは、目的又は用途毎にカードを用意して、複数のカードを使い分ける必要がある。

【０００７】最近では、非接触方式のＩＣカードが普及してきている。例えばキャッシュ･ディスペンサやコンサート会場の出入口、駅の改札口などに設置されたＩＣカード･リーダ／ライタは、利用者がかざしたＩＣカードに非接触でアクセスすることができる。ここで、利用者が暗証番号やパスワードをＩＣカード･リーダ側に入

力して、入力された暗証番号やパスワードをＩＣカード上に格納された暗証番号やパスワードと照合することで、ＩＣカードとＩＣカード･リーダ／ライタ間で本人確認又は認証処理が行なわれる。そして、本人確認又は認証処理に成功した場合には、例えば、ＩＣカード内に保存されているアプリケーションの利用が可能となる。ここで、ＩＣカードが保持するアプリケーションとしては、例えば、電子マネーや電子チケットなどの価値情報を挙げることができる。

【０００８】また、最近では、微細化技術の向上とも相俟って、比較的大容量の記憶空間を持つＩＣカードが出現し、普及してきている。従来のキャッシュ･カードなどにおいては単一の記憶領域すなわち単一のアプリケーションしか担持しないので、各用途又は目的毎に応じた複数のカードを持ち歩く必要ができる。これに対して、このような大容量メモリ付きのＩＣカードによれば、複数のアプリケーションを同時に格納しておくことができるので、１枚のＩＣカードを複数の用途に利用することができる。例えば、１枚のＩＣカード上に、電子決済を行なうための電子マネーや、特定のコンサート会場に入場するための電子チケットなど、２以上のアプリケーションを格納しておき、１枚のＩＣカードをさまざまな用途に適用させることができる。

【０００９】さらに、このような大容量メモリ機能付きのＩＣカード（又は、ＩＣカード機能が半導体チップ化されたＩＣチップ）を、携帯電話機などの携帯端末上に搭載することによって、利用者は携帯端末を所持しておくことで、電子決済を始めとする外部との電子的な価値情報のやり取りを行なうことができる。

【００１０】従来のキャッシュ･カードは単一の用途しか持たないので（前述）、キャッシュ･カード上の磁気ストライプは単一の暗証番号又はパスワードを持つことによってカード全体のセキュリティを管理することができた。

【００１１】これに対し、複数のアプリケーションを保持することができるメモリ機能付きＩＣカードや、このようなＩＣカード（又はＩＣチップ）を搭載した携帯端末においては、アプリケーション毎にアクセス権を制御する必要がある。何故ならば、唯１つの暗証コードのみで、ＩＣカード上のすべてのアプリケーションへのアクセスを開放してしまうと、例えば紛失時や盗難時におけるセキュリティが著しく低下するからである。

【００１２】

【発明が解決しようとする課題】本発明の目的は、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたＩＣチップを搭載した優れた携帯端末及びその制御方法、並びに、メモリ機能を備えた優れたＩＣカードを提供することにある。

【００１３】本発明の更なる目的は、ＩＣチップ上のメモリ領域に１以上のアプリケーションが割り当てられた優れた携帯端末及びその制御方法、並びに、メモリ領域に１以上のアプリケーションが割り当てた優れたＩＣカードを提供することにある。

【００１４】本発明の更なる目的は、ＩＣチップ上のメモリ領域に割り当てられた各アプリケーション毎にアクセス権を制御することができる、優れた携帯端末及びその制御方法、並びに、メモリ領域に割り当てられた各アプリケーション毎にアクセス権を制御することができる優れたＩＣカードを提供することにある。

【００１５】

【課題を解決するための手段及び作用】本発明は、上記課題を参酌してなされたものであり、その第１の側面は、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたＩＣチップを搭載した携帯端末であって、前記ＩＣチップ上のメモリ領域に割り当てられた、暗証コードによりアクセス権が制御された１以上のアプリケーションと、前記ＩＣチップが外部機器と無線通信するための無線インターフェースと、前記携帯端末内で前記ＩＣチップと有線通信するための有線インターフェースと、ユーザが暗証コードやその他のデータを入力することができるユーザ入力手段と、前記ユーザ入力手段から入力された暗証コード前記有線インターフェースを介して前記ＩＣチップに転送して、前記ＩＣチップ上のメモリ領域に割り当てられた各アプリケーションの暗証コードと比較照合する照合手段と、前記照合手段による比較照合の結果、暗証コードが一致するアプリケーションに関するアクセス権をユーザに与えるアクセス権制御手段と、を具備することを特徴とする携帯端末である。

【００１６】ここで言う携帯端末とは、例えば、携帯電話機や、ＰＤＡ（Personal DigitalAssistant）などのような、小型且つ軽量に構成されて、ユーザが絶えず持ち歩くことができる情報処理装置のことを指す。

【００１７】ＩＣチップにアンテナを搭載してクレジットカード・サイズ大に構成されたカートリッジのことを、一般に、「ＩＣカード」と呼ばれる。ＩＣチップは、携帯電話機やＰＤＡなどの携帯端末や、その他の情報処理装置に内蔵して用いるられる。また、ＩＣカードを情報処理装置に挿入して使用することもある。ＩＣチップ若しくはＩＣカードの使用形態としては、プリペイド形式の電子マネーや電子チケットなどの価値情報に関する機能が挙げられる。ＩＣチップ又はＩＣカードによって提供される機能のことを、以下では、「アプリケーション」とも呼ばれる。

【００１８】本発明の第１の側面に係る携帯端末上に搭載されたＩＣチップは、リーダ／ライタなどの外部機器と無線接続するための無線インターフェースと、搭載された携帯端末側のコントローラなどと内部接続するための有線インターフェースを備えており、リーダ／ライタと無線接続されたことに応答して、其処から届く電波に

より駆動可能となる。

【００１９】また、本発明の第１の側面に係る携帯端末上に搭載されたＩＣチップは、比較的大容量メモリのメモリ領域を備えている。このメモリ領域上には、１以上のアプリケーションが割り当てられている。各アプリケーションのアクセス権は、暗証番号やパスワードなどの暗証コードによって制御される。ここで言うアプリケーションには、電子マネーや電子チケットなどの価値情報が含まれる。

【００２０】リーダ／ライタなどの外部機器に無線接続した状態では、リーダ／ライタ上で入力された暗証コードが無線インターフェースでＩＣチップに入力することができる。また、携帯端末上のキーボードなどのユーザ入力装置上から入力された暗証コードは、有線インターフェース経由でＩＣチップに入力することができる。そして、無線インターフェース又は有線インターフェースから入力された暗証コードを比較照合して、その一致により、該当するアプリケーションへのアクセス権が与えられる。

【００２１】本発明の第１の側面によれば、まず、携帯端末上で所望のアプリケーションの暗証コードを入力しておいてから、リーダ／ライタのような外部機器に携帯端末をかざすことによって、そのまま外部機器上でアプリケーションを使用する（例えば、電子決済を行なう）ことができる。したがって、ユーザは、操作が不慣れな外部機器上のユーザ･インターフェースではなく、操作が手慣れた自分の携帯端末上で暗証コードを入力操作して、照合処理を受けることができる。すなわち、ＩＣチップを内蔵した情報処理機器上で暗証コードを入力してロックを解除後に外部機器と無線接続して、メモリ領域へのアクセスを許容するようにしてもよい。勿論、情報処理機機内のＩＣチップと外部機器との無線接続を確立した後、外部機器上で入力される暗証コードを基にアクセス権を制御するようにしてもよい。

【００２２】前記アクセス権制御手段は、アクセス権が与えられたアプリケーションに対する外部機器からの前記無線インターフェースを介した無線通信によるアクセスを許容するようにしてもよい。

【００２３】また、前記アクセス権制御手段は、前記無線インターフェース経由で接続された外部機器からの電波を検出しなくなったことに応答して、アクセス権を付与したアプリケーションに関する一連のトランザクションが終了したと判断して、トランザクション終了処理を行なうようにしてもよい。したがって、使用後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【００２４】また、前記アクセス権制御手段は、前記ＩＣチップから前記無線インターフェース経由で送出したコマンドに対するレスポンスが所定時間内に受信されなかったことに応答して、前記無線インターフェース経由で接続された外部機器と前記ＩＣチップとの一連のトランザクションが正常又は異常終了したとみなして、終了処理を行なうようにしてもよい。したがって、外部機器との無線接続が断たれた後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【００２５】本発明の第１の側面に係る携帯端末は、アプリケーション毎にあらかじめ暗証コードを登録する暗証コード登録手段と、プログラム起動手段と、起動されたプログラムに応じて該当するアプリケーションに対応する暗証コードを前記有線インターフェース経由で前記ＩＣチップに入力する暗証コード入力手段とをさらに備えていてもよい。このような場合、ユーザがディスプレイに表示されたメニュー画面などを介して所望のプログラムを選択して、携帯端末上で該当するプログラムが呼び出される。そして、起動されたプログラムに応答して、対応するアプリケーションについての暗証コードが前記有線インターフェース経由でＩＣチップに入力されてアクセス権を与えることができる。したがって、ユーザは、使用したいアプリケーションの暗証コードを入力する作業を省略することができ、操作性が向上する。

【００２６】また、前記ＩＣチップは、前記無線インターフェース経由で外部機器に接続されて給電されたことに応答して、前記ＩＣチップ上のメモリ領域にアクセスするために暗証コードの入力が必要である旨を前記有線インターフェース経由で通知するようにしてもよい。ＩＣチップを搭載した携帯端末上では、この通知に応答して、ディスプレイ上にダイアログを出現させたり、警告音を発して、ユーザに知らせることができる。したがって、ユーザは、携帯端末をリーダ／ライタなどの外部機器にかざしてアプリケーションを利用したいときに、暗証コードを入力する必要があるということを、確実に思い出すことができるので、ユーザの日常生活の各局面においてアプリケーションの使用が円滑化する。

【００２７】また、本発明の第２の側面は、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたＩＣチップを搭載した携帯端末の制御方法であって、前記携帯端末は、前記ＩＣチップが外部機器と無線通信するための無線インターフェースと、前記携帯端末内で前記ＩＣチップと有線通信するための有線インターフェースとを備え、前記ＩＣチップ上のメモリ領域には暗証コードによりアクセス権が制御された１以上のアプリケーションが割り当てられており、ユーザから暗証コードを入力するユーザ入力ステップと、前記ユーザ

入力ステップにより入力された暗証コードを前記有線インターフェース経由で前記ＩＣチップに送出するステップと、前記ＩＣチップ上のメモリ領域に割り当てられた各アプリケーションの暗証コードと、前記ユーザ入力ステップにより入力された暗証コードとを比較照合する照合ステップと、前記照合ステップにおける比較照合の結果、暗証コードが一致するアプリケーションに関するアクセス権をユーザに与えるアクセス権制御ステップと、を具備することを特徴とする携帯端末の制御方法である。

【００２８】本発明の第２の側面に係る携帯端末上に搭載されたＩＣチップは、リーダ／ライタなどの外部機器と無線接続するための無線インターフェースと、搭載された携帯端末側のコントローラなどと内部接続するための有線インターフェースを備えており、リーダ／ライタと無線接続されたことに応答して、その電波により駆動可能となる。

【００２９】また、本発明の第２の側面に係る携帯端末上に搭載されたＩＣチップは、比較的大容量メモリのメモリ領域を備えている。このメモリ領域上には、１以上のアプリケーションが割り当てられている。各アプリケーションのアクセス権は、暗証番号やパスワードなどの暗証コードによって制御される。ここで言うアプリケーションには、電子マネーや電子チケットなどの価値情報が含まれる。

【００３０】リーダ／ライタなどの外部機器に無線接続した状態では、リーダ／ライタ上で入力された暗証コードが無線インターフェースでＩＣチップに入力することができる。また、携帯端末上のキーボードなどのユーザ入力装置上から入力された暗証コードは、有線インターフェース経由でＩＣチップに入力することができる。そして、無線インターフェース又は有線インターフェースから入力された暗証コードを比較照合して、その一致により、該当するアプリケーションへのアクセス権が与えられる。

【００３１】本発明の第２の側面によれば、まず、携帯端末上で所望のアプリケーションの暗証コードを入力しておいてから、リーダ／ライタのような外部機器に携帯端末をかざすことによって、そのまま外部機器上でアプリケーションを使用する（例えば、電子決済を行なう）ことができる。したがって、ユーザは、操作が不慣れな外部機器上のユーザ・インターフェースではなく、操作が手慣れた自分の携帯端末上で暗証コードを入力操作して、照合処理を受けることができる。

【００３２】ここで、前記アクセス権制御ステップでは、アクセス権が与えられたアプリケーションに対する外部機器からの前記無線インターフェースを介した無線通信によるアクセスを許容するようにしてもよい。

【００３３】また、前記アクセス権制御ステップでは、前記無線インターフェース経由で接続された外部機器からの電波を検出しなくなったことに応答して、アクセス権を付与したアプリケーションに関する一連のトランザクションが終了したと判断して、トランザクション終了処理を行なうようにしてもよい。したがって、使用後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【００３４】また、前記アクセス権制御ステップでは、前記ＩＣチップから前記無線インターフェース経由で送出したコマンドに対するレスポンスが所定時間内に受信されなかったことに応答して、前記無線インターフェース経由で接続された外部機器と前記ＩＣチップとの一連のトランザクションが正常又は異常終了したとみなして、終了処理を行なうようにしてもよい。したがって、外部機器との無線接続が断たれた後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【００３５】本発明の第２の側面に係る携帯端末の制御方法は、アプリケーション毎にあらかじめ暗証コードを登録する暗証コード登録ステップと、プログラム起動手段と、起動されたプログラムに応じて該当するアプリケーションに対応する暗証コードを前記有線インターフェース経由で前記ＩＣチップに入力する暗証コード入力ステップとをさらに備えていてもよい。このような場合、ユーザがディスプレイに表示されたメニュー画面などを介して所望のプログラムを選択して、携帯端末上で該当するプログラムが呼び出される。そして、起動されたプログラムに応答して、対応するアプリケーションについての暗証コードが前記有線インターフェース経由でＩＣチップに入力されてアクセス権を与えることができる。このような場合、ユーザは、使用したいアプリケーションの暗証コードを入力する作業を省略することができ、操作性が向上する。

【００３６】また、前記ＩＣチップが前記無線インターフェース経由で外部機器に接続されて給電されたことに応答して、前記ＩＣチップ上のメモリ領域にアクセスするために暗証コードの入力が必要である旨を前記有線インターフェース経由で通知するステップをさらに備えていてもよい。携帯端末上では、この通知に応答して、ディスプレイ上にダイアログを出現させたり、警告音を発して、ユーザに知らせることができる。したがって、ユーザは、携帯端末をリーダ／ライタなどの外部機器にかざしてアプリケーションを利用したいときに、暗証コードを入力する必要があるということを、確実に思い出す

ことができるので、ユーザの日常生活の各局面においてアプリケーションの使用が円滑化する。

【００３７】また、本発明の第３の側面は、携帯端末に付随して使用されるＩＣカードであって、外部機器と無線通信するための無線インターフェースと、前記携帯端末と有線通信するための有線インターフェースと、暗証コードによりアクセス権が制御された１以上のアプリケーションが割り当てられたメモリ領域と、を具備し、前記無線インターフェース経由で外部機器に接続されたことに応答して給電されて駆動する、ことを特徴とするＩＣカードである。

【００３８】そして、前記無線インターフェース経由で受信した暗証コードが一致したことに応答して、メモリ領域上の対応するアプリケーションのアクセス権が前記無線インターフェース経由で接続された外部機器に与えられる。

【００３９】あるいは、前記有線インターフェース経由で受信した暗証コードが一致したことに応答して、メモリ領域上の対応するアプリケーションのアクセス権が前記無線インターフェース経由で接続された外部機器に与えられる。このような場合、まず、携帯端末上で所望のアプリケーションの暗証コードを入力しておいてから、リーダ／ライタのような外部機器に携帯端末をかざすことによって、そのまま外部機器上でアプリケーションを使用する（例えば、電子決済を行なう）ことができる。したがって、ユーザは、操作が不慣れな外部機器上のユーザ･インターフェースではなく、操作が手慣れた自分の携帯端末上で暗証コードを入力操作して、照合処理を受けることができる。

【００４０】本発明の第３の側面に係るＩＣカードは、前記無線インターフェース経由で接続された外部機器からの電波を検出しなくなったことに応答して、該外部機器に与えられているアプリケーションへのアクセス権が失効するようにしてもよい。したがって、使用後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【００４１】また、本発明の第３の側面に係るＩＣカードは、前記無線インターフェース経由で送出したコマンドに対するレスポンスが所定時間内に受信されなかったことに応答して、該外部機器に与えられているアプリケーションへのアクセス権が失効するようにしてもよい。したがって、外部機器との無線接続が断たれた後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【００４２】また、本発明の第３の側面に係るＩＣカードは、前記無線インターフェース経由で外部機器に接続されて給電されたことに応答して、前記ＩＣチップ上のメモリ領域にアクセスするために暗証コードの入力が必要である旨を前記有線インターフェース経由で通知するようにしてもよい。ＩＣカードが付随する携帯端末上では、この通知に応答して、ディスプレイ上にダイアログを出現させたり、警告音を発して、ユーザに知らせることができる。したがって、ユーザは、携帯端末をリーダ／ライタなどの外部機器にかざしてアプリケーションを利用したいときに、暗証コードを入力する必要があるということを、確実に思い出すことができるので、ユーザの日常生活の各局面においてアプリケーションの使用が円滑化する。

【００４３】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００４４】

【発明の実施の形態】以下、図面を参照しながら本発明の実施例を詳解する。

【００４５】図１には、本発明の一実施形態に係る携帯端末１０のハードウェア構成を模式的に示している。携帯端末１０は、例えば、携帯電話機やＰＤＡ（Personal Digital Assistant）などのような、小型且つ軽量に構成されて、ユーザが常に持ち運ぶことができる情報処理端末である。

【００４６】図示の携帯端末１０は、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたＩＣチップ５０を搭載するとともに、携帯端末１０内の動作を統括的に制御するコントローラ１１と、ユーザが暗証番号やパスワードを始めとする各種の文字列やコマンドを入力するためのキー／ボタンなどからなるユーザ入力装置１２と、処理結果を画面表示するための液晶ディスプレイ（ＬＣＤ：liquid Crystal Display）などの表示装置１３を備えている。もちろん、携帯端末１０としての本来の機能を実現するために、図示する以外の周辺装置や回路コンポーネントを備えていてもよい。

【００４７】ここで、ＩＣチップにアンテナを搭載してクレジットカード・サイズ大に構成されたカートリッジのことを、一般に、「ＩＣカード」と呼ばれる。

【００４８】また、携帯端末１０がＩＣチップ５０を装備する形態は一意ではない。例えば、半導体チップの形態のＩＣを無線アンテナとともに内蔵するようにしてもよいし、カード状に構成されたＩＣチップすなわちＩＣカードを、携帯端末１０に配設されたカード・スロットなどに挿入して用いるようにしてもよい。ＩＣチップ若しくはＩＣカードの使用形態としては、プリペイド形式の電子マネーや電子チケットなどの価値情報に関する機能が挙げられる。ＩＣチップ又はＩＣカードによって提供される機能のことを、以下では、「アプリケーショ

ン」とも呼ぶ。

【００４９】コントローラ１１は、ＣＰＵ（Central Processing Unit），ＲＯＭ（Read Only Memory），ＲＡＭ（Random Access Memory）などを一体化して構成される。コントローラ１１は、ＲＯＭ上に格納されたプログラム･コードを実行することによって、携帯端末１０内の各種オペレーションを制御する。

【００５０】ＩＣチップ５０は、外部機器１００と無線接続するための無線インターフェース１４と、携帯端末１０側のコントローラ１１と有線接続するための有線インターフェース１５を備えている。無線インターフェース１４に関しては、例えば、ＩＳＯ　７８１６で定義された接触インターフェース規格、又は、ＩＳＯ　１４４４３で定義された無線インターフェース規格を使用することができる。ＩＣチップ５０と外部機器１００との接続方式に関しては、後述に譲る。

【００５１】ＩＣチップ５０は、例えば、非接触ＩＣカードの技術が適用されており、無線インターフェース１４経由で受信される外部機器１００からの電波によって駆動する。言い換えれば、ユーザが外部機器１００に携帯端末１０をかざしていない状態では、外部機器１００からの電波が届かなくなり、ＩＣチップ５０の動作は減勢されてしまう。本実施形態では、電波が途切れることに応答して、ＩＣチップ５０内部へのアクセス権は消失する（後述）。

【００５２】また、本実施形態に係るＩＣチップ５０は、比較的大容量のメモリ領域を備えている。このようなメモリ領域は、微細化技術などによりもたらされる。メモリ領域は、半導体メモリや磁気ストライプ、あるいは読み書き可能なその他の記憶媒体で構成される。このメモリ領域上には、１以上のアプリケーションが割り当てられている。ここで言うアプリケーションの例としては、電子マネーや電子チケットを始めとする価値情報を挙げることができる。

【００５３】この種の価値情報を無断使用や盗用から保護するために、各アプリケーション毎に暗証番号やパスワードなどの暗証コードを設定することによって、アプリケーション単位でメモリ領域へのアクセス権が制御されている。例えば、無線インターフェース１４や有線インターフェース１５を介して入力された暗証コードと各アプリケーションが持つ暗証コードとを比較照合して、一致するアプリケーションについてのアクセス権が与えられる（後述）。

【００５４】外部機器１００は、ＩＣチップ５０のメモリ領域に割り当てられているアプリケーションを利用する装置であり、例えば非接触ＩＣカードの技術を適用して、ＩＣチップ５０と無線接続するためのリーダ／ライタ１０１を含んでいる。勿論、外部機器１００は、それ以外にも、特定業務用の演算処理を行なう回路コンポーネントや周辺装置類、ユーザとの対話入力を行うための表示装置並びに入力装置（いずれも図示しない）を装備している。

【００５５】外部機器１００は、例えば、銀行内のＡＴＭ（Automatic Teller Machine）端末のような電子マネーを使用する装置や、コンサート会場のゲートや駅や空港の改札口など電子チケットを使用する装置など電子的な価値情報を処理する装置、さらには、宿泊施設のセーフティ･ボックスのように本人確認又は認証処理を行なう装置である。

【００５６】図１に示すようなシステム構成によれば、ユーザは携帯端末１０上のユーザ入力装置１２から暗証コードを入力して、ロックを解除する。場合によってはユーザから入力された値を表示装置１３上で確認して、携帯端末１０に内蔵されたＩＣチップ５０に入力された暗証コードを有線インターフェース１５経由で送出する。そして、ＩＣチップ５０内では、メモリ領域上の各アプリケーション又は各ディレクトリに設定されている暗証コードとユーザ入力された暗証コードの照合が行なわれる。そして、一致するアプリケーション又はディレクトリに割り当てられたメモリ領域へのアクセス権がユーザに与えられる。あるいは、携帯端末１０内のＩＣチップ５０と外部機器１００との無線接続を確立した後、外部機器１００上で入力される暗証コードを基に、アプリケーションへのアクセス権を制御するようにしてもよい。

【００５７】リーダ／ライタ１０１とＩＣチップ５０との無線通信は、例えば電磁誘導の原理に基づいて実現される。図２には、電磁誘導に基づくリーダ／ライタ１０１とＩＣチップ５０との無線通信の仕組みを概念的に図解している。リーダ／ライタ１０１は、ループ･コイルで構成されたアンテナ$L_{RW}$を備え、このアンテナ$L_{RW}$に電流$I_{RW}$を流すことでその周辺に磁界を発生させる。一方、ＩＣチップ５０側では、電気的にはＩＣチップ５０の周辺にループ･コイル$L_c$が形設されている。ＩＣチップ５０側のループ･コイル$L_c$端にはリーダ／ライタ１０１側のループ・アンテナ$L_c$が発する磁界による誘導電圧が生じ、ループ･コイル$L_c$端に接続されたＩＣチップ５０の端子に入力される。

【００５８】リーダ／ライタ１０１側のアンテナ$L_{RW}$とＩＣチップ５０側のループ･コイル$L_c$は、その結合度は互いの位置関係によって変わるが、系としては１個のトランスを形成していると捉えることができ、図３に示すようにモデル化することができる。

【００５９】リーダ／ライタ１０１は、アンテナ$L_{RW}$に流す電流$I_{RW}$を変調することで、ＩＣカード上のループ･コイル$L_c$に誘起される電圧Ｖ0は変調を受け、そのことを利用してリーダ／ライタ１０１はＩＣチップ５０へのデータ送信を行うことができる。ここで言う送信データには、外部機器１００側でユーザ入力された暗証番号やパスワードなどの、アプリケーションのアクセス権を

得るための暗証コードや、電子マネーや電子チケットなどのアプリケーションが提供する価値情報が含まれる。

【００６０】また、ＩＣチップ５０は、リーダ／ライタ１０１へ返送するためのデータに応じてループ･コイル$L_c$の端子間の負荷を変動させる機能（Load Switching）を持つ。ループ･コイル$L_c$の端子間の負荷が変動すると、リーダ／ライタ１０１側ではアンテナ端子間のインピーダンスが変化して、アンテナ$L_{RW}$の通過電流$I_{RW}$や電圧$V_{RW}$の変動となって現れる。この変動分を復調することで、リーダ／ライタ１０１はＩＣチップの返送データを受信することができる。外部機器１００がＩＣチップ５０から受信するデータには、電子マネーや電子チケットなどのアプリケーションが提供する価値情報が含まれる。

【００６１】図４には、本実施形態に係る携帯端末１０に内蔵されるＩＣチップ５０内の機能構成を図解している。

【００６２】同図に示すように、ＩＣチップ５０は、外部機器１００側のリーダ／ライタ１０１と無線通信を行うアンテナが接続されるＲＦ部５１と、例えば購入済みチケット情報や銀行の預金者情報（電子マネー）などのアプリケーション毎に割り当てられた記憶領域を持つメモリ５２と、暗証コードの比較照合を行う照合部５３と、有線インタフェース５４と、これらの構成部品を統括的にコントロールする制御部５５とからなる。

【００６３】制御部５５は、ＣＰＵ（Central Processing Unit），ＲＯＭ（Read Only Memory），ＲＡＭ（Random Access Memory）などを一体化して構成されている。制御部５５は、ＲＯＭに格納されたプログラム･コードを実行することによって、ＩＣチップ５０内の動作を制御する。また、制御部５５は、有線インターフェース５４を介して、携帯端末１０側のコントローラ１１と通信することができる。

【００６４】メモリ５２は、アプリケーション毎に領域が割り当てられている。図示の例では、メモリ５２上には、アプリケーションＡ、アプリケーションＢ、アプリケーションＣの各々に領域が割り当てられている。さらに、必要に応じて各アプリケーション毎に、本人確認又は認証処理用の暗証コードが設定されている。アプリケーションに割り当てられた領域内には、暗証コードを保存する暗証コード領域が含まれる。

【００６５】なお、メモリ５２は、半導体メモリの他、磁気ストライプなど、読み書き可能な記憶媒体であればよく、特定のデバイスには限定されない。

【００６６】本実施形態においては、有線インタフェース５４を通して送られてくる暗証コードを、照合部５３において、各アプリケーションに割り当てられたメモリ領域に設定されている暗証コードと照合して、一致するされたメモリ領域に対するアクセスを許可する。アクセスが許可されたメモリ領域は、ＲＦ部５１を介してリーダ／ライタ１０１から読み書きが可能となる。

【００６７】有線インタフェース５４を通して送られてくる暗証コードとは、要するに、携帯端末１０上でユーザ入力された暗証コードのことである。すなわち、本実施形態によれば、ユーザは、操作が不慣れな外部機器１００上のユーザ･インターフェースではなく、操作が手慣れた自分の携帯端末１０上で暗証コードを入力操作して照合処理を受けることができる。

【００６８】図５には、携帯端末１０上のユーザ入力装置１１から入力された暗証コードの照合処理によりメモリ５２に割り当てられたアプリケーションのアクセス許可を行うための処理手順をフローチャートの形式で示している。以下、図５に示すフローチャートを参照しながら、アプリケーションのアクセス許可手続について説明する。

【００６９】まず、ユーザは、携帯端末１０上のユーザ入力装置１１を使って、暗証コードを入力する（ステップＳ１）。

【００７０】このように入力された暗証コードは、有線インターフェース５２を介して、ＩＣチップ５０内の照合部５３に転送される（ステップＳ２）。

【００７１】次いで、照合部５３は、メモリ５２に割り当てられた各アプリケーションに対して設定されている暗証コードと、ユーザ入力装置１２を介して入力された暗証コードとを比較照合する（ステップＳ３）。

【００７２】そして、比較照合の結果、暗証コードが一致するアプリケーションに関するアクセス権がユーザに与えられる（ステップＳ４）。アクセス権が与えられたアプリケーションに割り当てられた記憶領域は、リーダ／ライタ１０１側からは無線通信によりアクセスすることが可能となる。

【００７３】勿論、照合部５３は、有線インターフェース５４経由で受け取られた（すなわち携帯端末１０上でユーザ入力された）暗証コードを照合処理するだけでなく、ＲＦ部５１経由で受信された（すなわち、外部機器１００上でユーザ入力された）暗証コードを照合処理することもできる。

【００７４】また、アクセス許可後のリーダ／ライタ１０１との一連のトランザクションが終了したら、それを制御部５５がこれを解釈して、有線インタフェース５４を通して通知する。

【００７５】あるいは、制御部５５は、トランザクションの正常あるいは異常終了の後、有線インタフェース５４からのコマンドを待つか、又は、携帯端末１０本体の電源がＯＦＦにされる（すなわち、リーダ／ライタ５０側からの電波が途絶えて減勢される）のを待つ。この場合は、このＩＣチップ５０を搭載する携帯端末１０側のコントローラ１１が所定時間が経過した後に、ＩＣチップ５０に対して次のコマンドを送るか、又はＩＣチップ５０の電源をＯＦＦにするなどの終了処理を行う。

【００７６】図６には、外部機器５０からの送信電波の検出結果によりアプリケーションのアクセス権を制御する処理手続をフローチャートの形式で示している。以下、このフローチャートに従って、アプリケーションのアクセス権制御について説明する。

【００７７】ＲＦ部５１経由で外部機器１００と無線接続されている期間中、制御部５５は、ＲＦ部５１を介して電波を受信しているか否かを常にチェックしている（ステップＳ１１）。

【００７８】そして、電波が検出されなくなると、ＲＦ部５１経由で無線接続されている外部機器１００とＩＣチップ５０との一連のトランザクションが終了したと判断する（ステップＳ１２）。

【００７９】そして、制御部５５は、外部機器１００とのトランザクションの終了処理を行なう（ステップＳ１３）。この結果、外部機器１００に与えられていたアプリケーションへのアクセス権は消滅する。

【００８０】この結果、使用後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末１０を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【００８１】また、図７には、ＩＣチップ５０からの送信コマンドに対する外部機器１００からのレスポンスによりアプリケーションのアクセス権を制御する処理手続をフローチャートの形式で示している。以下、このフローチャートに従って、アプリケーションのアクセス権制御について説明する。

【００８２】制御部５５は、ＲＦ部５１を介して外部機器１００にコマンドを送信すると（ステップＳ２１）、これに対するレスポンスが返されたか否かをチェックする（ステップＳ２２）。

【００８３】そして、コマンドを送信してから所定期間内にレスポンスが受信されなかった場合には（ステップＳ２３）、ＩＣチップ５０と外部機器１００との一連のトランザクションが正常又は異常終了したと判断して（ステップＳ２４）、外部機器１００とのトランザクションの終了処理を行なう（ステップＳ２５）。

【００８４】この結果、外部機器１００との無線接続が断たれた後にアプリケーションのアクセス権が与えられたままの状態ではなくなるので、例えば携帯端末を紛失した場合や盗難に遭った場合に、アプリケーションが無断で使用されることはなくなる。したがって、ユーザは、電子マネーなどの価値情報の無断使用や盗用を免れることができる。

【００８５】また、ＩＣチップ５０は、有線インターフェース５４経由で暗証コードが入力される前に、ＲＦ部４１を通してリーダ／ライタ５５との間で無線通信を行い、外部機器１００との間でデータの送受信を行った後に、制御部５５がさらにデータの送受信を行う場合には暗証コードによる認証が必要であることを検出して、有線インタフェース５４を通してその旨を携帯端末１０側のコントローラ１１に通知する。

【００８６】図８には、ＩＣチップ５０がＲＦ部５１を介して外部機器１００に無線接続されたことに応答して、携帯端末側に暗証コードの入力を促すための処理手順をフローチャートの形式で示している。

【００８７】制御部５５は、ＩＣチップ５０がＲＦ部５１を介して外部機器１００に無線接続されたか否かを常にチェックする（ステップＳ３１）。

【００８８】そして、ＩＣチップ５０がＲＦ部５１経由で外部機器１００に接続されて給電されると、制御部５５は、有線インターフェース５４経由で、携帯端末１０のコントローラ１１に対して、メモリ５２にアクセスするために暗証コードの入力が必要である旨を通知する（ステップＳ３２）。

【００８９】携帯端末１０側では、この通知に応答して、警告音を発したり、あるいは、表示装置１２上にダイアログを出現させるなどして、ユーザに対して所望のアプリケーションを利用するための暗証コードの入力をプロンプトする。（ステップＳ３３）。

【００９０】したがって、ユーザは、携帯端末をリーダ／ライタなどの外部機器にかざしてアプリケーションを利用したいときに、暗証コードを入力する必要があるということを、確実に思い出すことができるので、ユーザの日常生活の各局面においてアプリケーションの使用が円滑化する。

【００９１】図９には、本発明の他の実施形態に係る携帯端末１０－２のハードウェア構成を模式的に示している。

【００９２】図示の携帯端末１０－２は、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたＩＣチップ５０を搭載するとともに、携帯端末１０内の動作を統括的に制御するコントローラ１１と、ユーザが暗証番号やパスワードを始めとする各種の文字列やコマンドを入力するためのキー／ボタンなどからなるユーザ入力装置１２と、処理結果を画面表示するための液晶ディスプレイ（ＬＣＤ：Liquid Crystal Display）などの表示装置１３を備えている。もちろん、携帯端末１０－２としての本来の機能を実現するために、図示する以外の周辺装置や回路コンポーネントを備えていてもよい。

【００９３】ＩＣチップ５０は、外部機器１００と無線接続するための無線インターフェース１４と、携帯端末１０側のコントローラ１１と有線接続するための有線インターフェース１５を備えている。無線インターフェース１４に関しては、例えば、ＩＳＯ　７８１６で定義された接触インターフェース規格、又は、ＩＳＯ　１４４４３で定義された無線インターフェース規格を使用する

ことができる（同上）。

【００９４】ＩＣチップ５０は、例えば、非接触ＩＣカードの技術が適用されており、無線インターフェース経由で受信される外部機器１００からの電波によって駆動する。言い換えれば、外部機器１００に携帯端末１０をかざしていない状態では、外部機器１００からの電波が届かないので、ＩＣチップ５０は減勢されて、ＩＣチップ５０内部へのアクセス権は消失する。

【００９５】また、ＩＣチップ５０は、比較的大容量のメモリ領域を備えている。このようなメモリ領域は、微細化技術などによりもたらされる。メモリ領域は、半導体メモリや磁気ストライプ、あるいは読み書き可能なその他の記憶媒体で構成される。このメモリ領域上には、１以上のアプリケーションが割り当てられている。ここで言うアプリケーションの例としては、電子マネーや電子チケットを始めとする価値情報を挙げることができる。

【００９６】この種の価値情報を無断使用や盗用から保護するために、各アプリケーション毎に暗証番号やパスワードなどの暗証コードによってアクセス権が制御されている。例えば、無線インターフェース１４や有線インターフェース１５を介して入力された暗証コードと各アプリケーションが持つ暗証コードとを比較照合して、一致するアプリケーションについてのアクセス権が与えられる。

【００９７】携帯端末１０－２は、図１で示された携帯端末内のコントローラ１１内に暗証コード記憶領域を備えたものである。したがって、あらかじめコントローラ１１内のプログラムに対応した暗証コードをこの暗証コード記憶領域に記憶しておくことによって、呼び出されたプログラムに応じて対応する暗証コードを有線インタフェース経由でＩＣチップ５０側に送出することができる。したがって、ユーザは、ＩＣチップ５０内に格納された同じアプリケーションを使用するために、暗証コードを逐次入力する必要がなくなり、機器の操作性が向上する。

【００９８】図１０には、プログラムの起動により暗証コードの入力を省略するための処理手続をフローチャートの形式で示している。

【００９９】まず、アプリケーション毎にあらかじめ暗証コードを登録する（ステップＳ４１）。登録された暗証コードは、コントローラ５５内の所定の暗証番号記憶領域に格納される。

【０１００】そして、ユーザは、アプリケーションを使用したい局面においては、例えば、表示装置１３上に表示されたメニューリスト（図示しない）を介して、所望のプログラムを選択する（ステップＳ４２）。

【０１０１】この結果、コントローラ１１は、選択されたプログラムを起動する（ステップＳ４３）。

【０１０２】そして、コントローラ１１は、この起動された起動されたプログラムに応じて該当するアプリケーションに対応する暗証コードを暗証コード記憶領域から読み出して、有線インターフェース１５経由でＩＣチップ５０に送出する（ステップＳ４４）。

【０１０３】この結果、ＩＣチップ内では、メモリ領域に割り当てられた各アプリケーションに対して設定されている暗証コードと、有線インターフェース１５経由で入力された暗証コードとを比較照合する（ステップＳ４５）。

【０１０４】そして、比較照合の結果、暗証コードが一致するアプリケーションに関するアクセス権がユーザに与えられる（ステップＳ４６）。アクセス権が与えられたアプリケーションに割り当てられた記憶領域は、リーダ／ライタ１０１が無線通信によりアクセスすることが可能となる。

【０１０５】このような場合、ユーザがディスプレイに表示されたメニュー画面などを介して所望のプログラムを選択して、携帯端末上で該当するプログラムが呼び出される。そして、起動されたプログラムに応答して、対応するアプリケーションについての暗証コードが前記有線インターフェース経由でＩＣチップに入力されてアクセス権を与えることができる。したがって、ユーザは、使用したいアプリケーションの暗証コードを入力する作業を省略することができるので、機器操作性が向上する。

【０１０６】［追補］以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。

【０１０７】本明細書中では、本発明に係るＩＣチップが携帯電話機やＰＤＡなどの携帯端末に内蔵して使用される場合を例にとって説明してきたが、本発明の要旨はこれに限定されない。例えば、スタンドアロンのＩＣカードとして使用する場合や他の機器に内蔵してＩＣチップを使用する場合においても、同様に本発明の効果を奏することができる。

【０１０８】要するに、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１０９】

【発明の効果】以上詳記したように、本発明によれば、外部機器との無線通信により給電されて駆動するとともにメモリ機能を備えたＩＣチップを搭載した優れた携帯端末及びその制御方法、並びに、メモリ機能を備えた優れたＩＣカードを提供することができる。

【０１１０】また、本発明によれば、ＩＣチップ上のメモリ領域に１以上のアプリケーションが割り当てることができる、優れた携帯端末及びその制御方法、並びに、

メモリ領域に１以上のアプリケーションが割り当てた優れたＩＣカードを提供することができる。

【０１１１】また、本発明によれば、ＩＣチップ上のメモリ領域に割り当てられた各アプリケーション毎にアクセス権を制御することができる、優れた携帯端末及びその制御方法、並びに、メモリ領域に割り当てられた各アプリケーション毎にアクセス権を制御することができる優れたＩＣカードを提供することができる。

【０１１２】本発明によれば、例えば携帯端末上に内蔵したＩＣチップを銀行用カードとして使用する場合において、使用者にとって使い慣れた携帯端末側で暗証番号を入力することによって、本人確認又は認証処理を受けることができる。この結果、不慣れな銀行のＡＴＭ端末に対する操作を最小限にすることができる。

【０１１３】また、本発明によれば、例えば銀行内のＡＴＭ端末に向かって携帯端末をかざすことによって、ＡＴＭ端末側から携帯端末に対して適切な暗証番号の入力を促すことができる。

【０１１４】また、本発明によれば、携帯端末内においてプログラムと暗証コードを結び付けておくことによって、例えば、ある銀行の残高表示プログラムが呼び出されたとき、自動的に暗証番号が呼び出される。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る携帯端末１０のハードウェア構成を模式的に示した図である。

【図２】電磁誘導に基づくリーダ／ライタ１０１とＩＣチップ５０との無線通信の仕組みを概念的に示した図である。

【図３】リーダ／ライタ１０１とＩＣチップ５０からなる系を１個のトランスとして捉えてモデル化した図である。

【図４】本実施形態に係る携帯端末１０に内蔵されるＩＣチップ５０内の機能構成を示した図である。

【図５】携帯端末１０上のユーザ入力装置１１から入力された暗証コードの照合処理によりメモリ５２に割り当てられたアプリケーションのアクセス許可を行うための処理手順を示したフローチャートである。

【図６】外部機器５０からの送信電波の検出結果によりアプリケーションのアクセス権を制御する処理手続を示したフローチャートである。

【図７】ＩＣチップ５０からの送信コマンドに対する外部機器１００からのレスポンスによりアプリケーションのアクセス権を制御する処理手続を示したフローチャートである。

【図８】ＩＣチップ５０がＲＦ部５１を介して外部機器１００に無線接続されたことに応答して、携帯端末側に暗証コードの入力を促すための処理手順を示したフローチャートである。

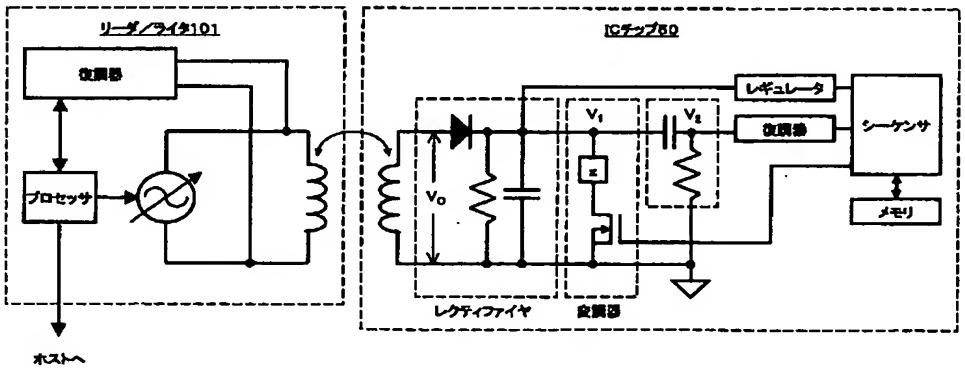
【図９】本発明の他の実施形態に係る携帯端末１０－２のハードウェア構成を模式的に示した図である。

【図１０】プログラムの起動により暗証コードの入力を省略するための処理手続を示したフローチャートである。

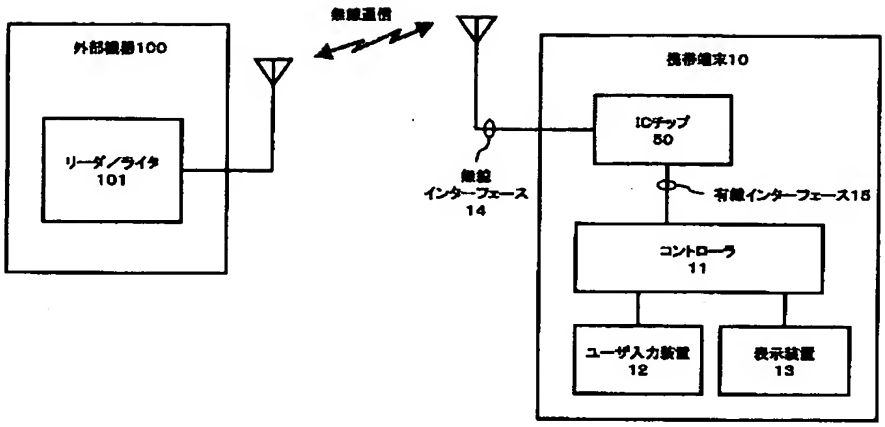
【符号の説明】

１０…携帯端末
１１…コントローラ
１２…ユーザ入力装置
１３…表示装置
１４…無線インターフェース
１５…有線インターフェース
５０…ＩＣチップ
５１…ＲＦ部
５２…メモリ
５３…照合部
５４…有線インターフェース
５５…制御部
１００…外部機器
１０１…リーダ／ライタ

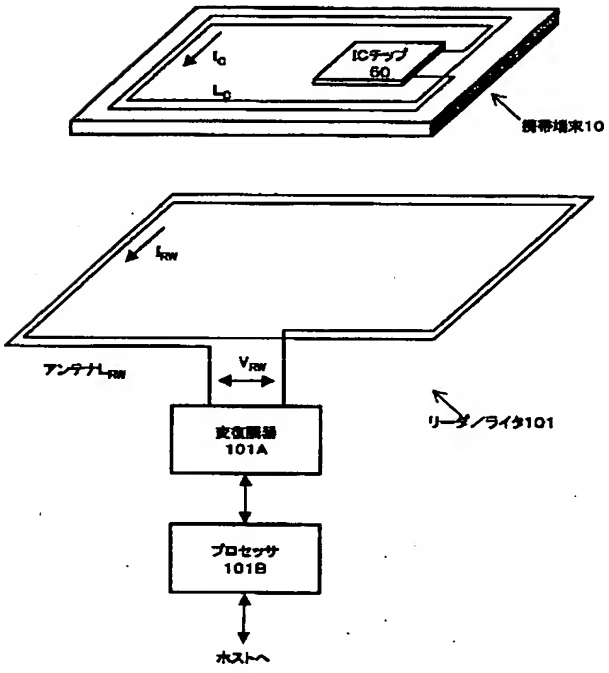
【図３】



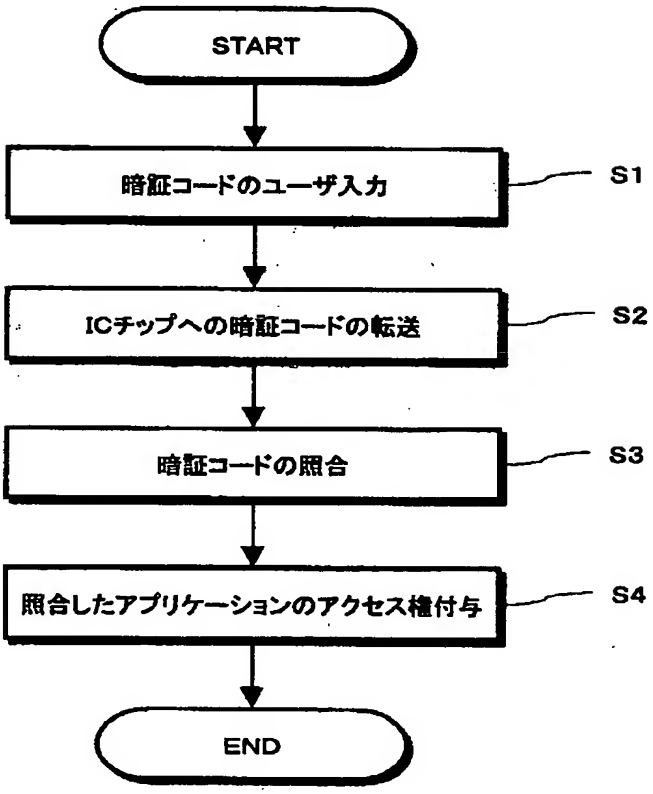
【図１】


外部機器100
リーダ／ライタ
101
無線通信
無線
インターフェース
14
携帯端末10
ICチップ
50
有線インターフェース15
コントローラ
11
ユーザ入力装置
12
表示装置
13

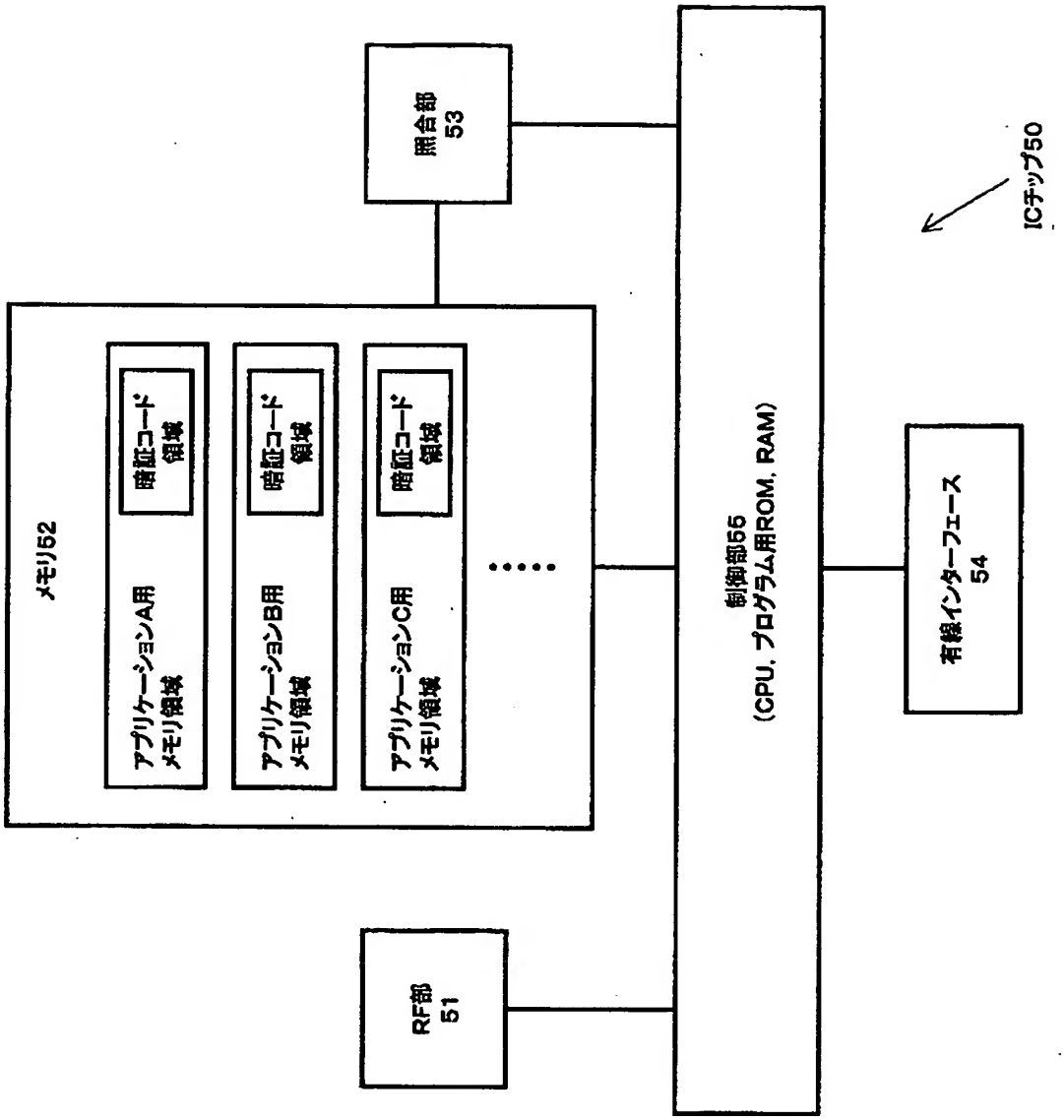
【図２】


ICチップ
50
携帯端末10
アンテナ
変復調器
101A
プロセッサ
101B
ホストへ
リーダ／ライタ101

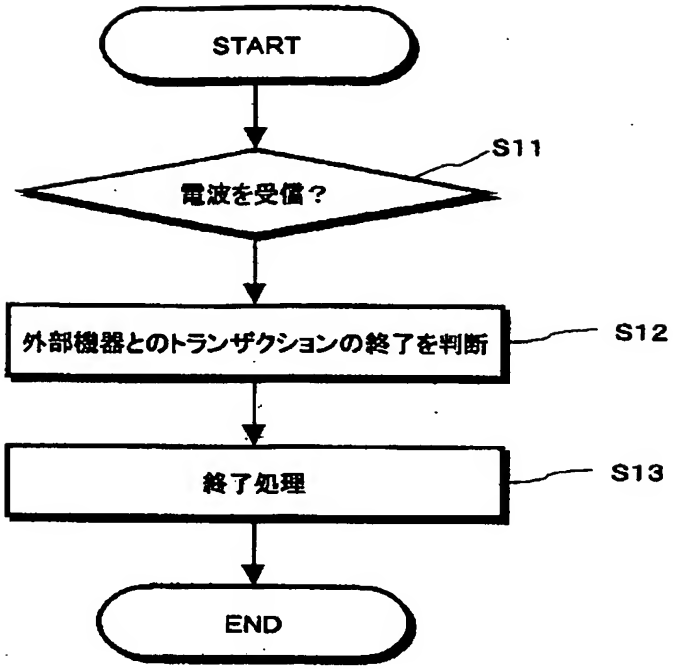
【図５】


START
暗証コードのユーザ入力
S1
ICチップへの暗証コードの転送
S2
暗証コードの照合
S3
照合したアプリケーションのアクセス権付与
S4
END

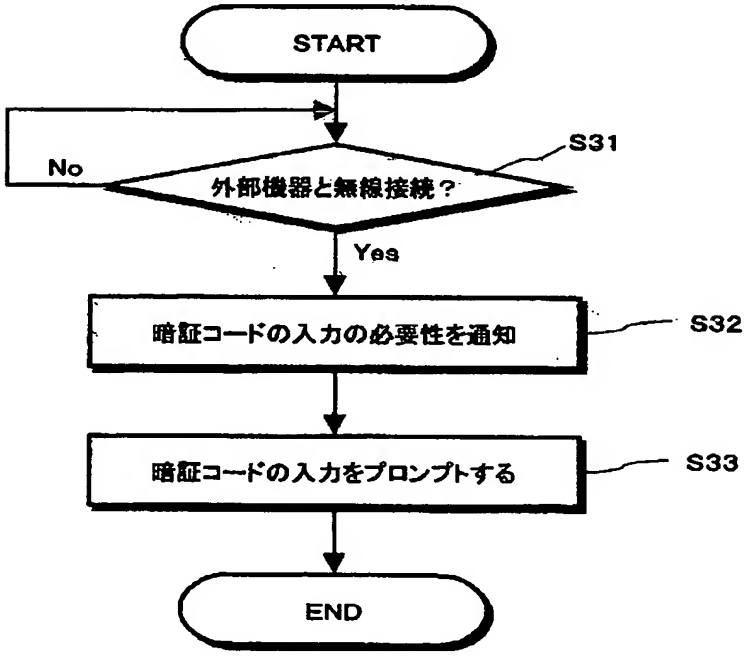
【図４】


ICチップ50
照合部
53
メモリ52
暗証コード
領域
アプリケーションA用
メモリ領域
暗証コード
領域
アプリケーションB用
メモリ領域
暗証コード
領域
アプリケーションC用
メモリ領域
制御部55
(CPU, プログラム用ROM, RAM)
有線インターフェース
54
RF部
51

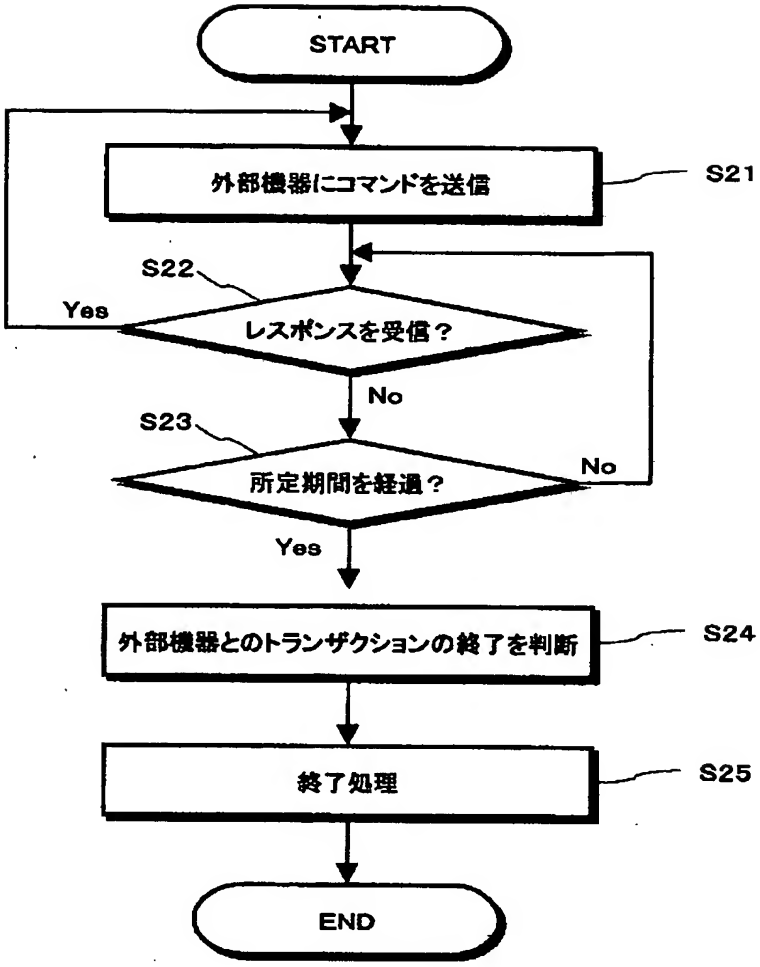
【図６】


START
S11
電波を受信？
外部機器とのトランザクションの終了を判断
S12
終了処理
S13
END

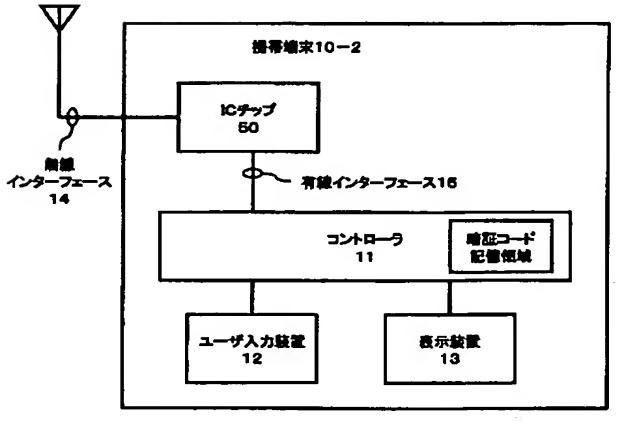
【図８】


START
S31
No
外部機器と無線接続？
Yes
暗証コードの入力の必要性を通知
S32
暗証コードの入力をプロンプトする
S33
END

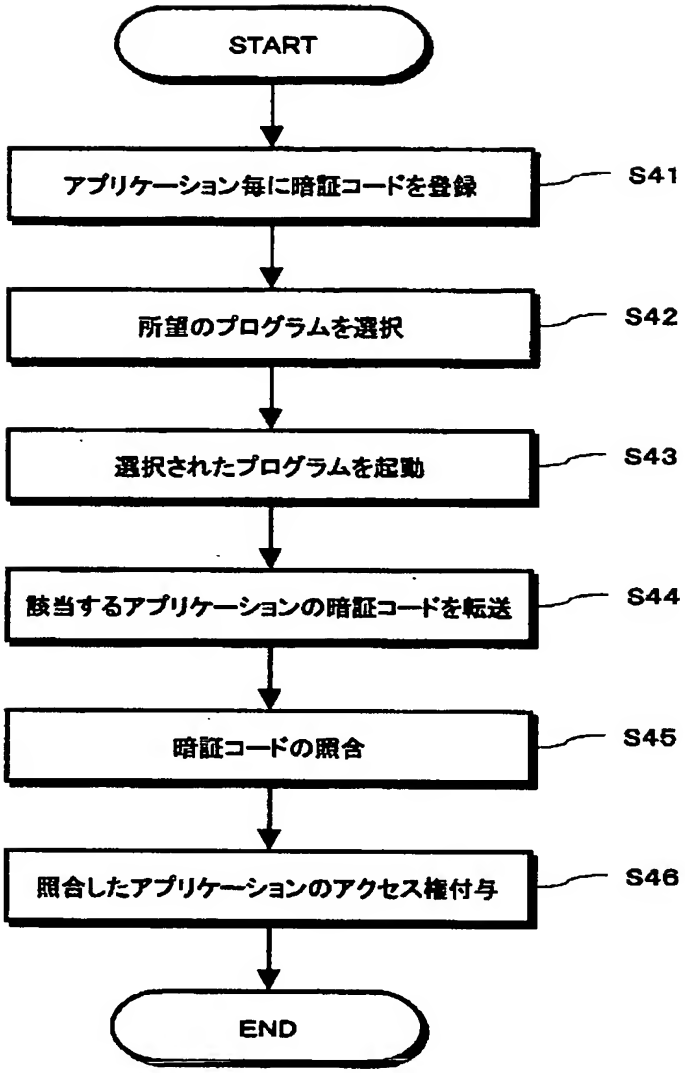
【図７】


START
外部機器にコマンドを送信
S21
S22
Yes
レスポンスを受信？
No
S23
所定期間を経過？
No
Yes
外部機器とのトランザクションの終了を判断
S24
終了処理
S25
END

【図９】


携帯端末10－2
ICチップ
50
無線
インターフェース
14
有線インターフェース16
コントローラ
11
暗証コード
記憶領域
ユーザ入力装置
12
表示装置
13

【図１０】




フロントページの続き

Ｆターム(参考) 2C005 MB08 NA08 NA09 SA02 SA05
SA12 SA22 SA25 TA21 TA22
5B017 AA03 BA05 CA14 CA15
5B035 AA06 AA13 BB09 BC00 CA12
CA23 CA38
5B082 EA12